CLAIMS

What is claimed is:

1   1.   A method for sending secure messages in a broadcast network

2   comprising the steps of:

3   encrypting data with a key;

4   hashing said key;

5   combining said encrypted data and said key in a broadcast

6   message; and

7   transmitting said broadcast message to a plurality of receiving

8   nodes.

1   2.   The method of claim 1 wherein the key is a plurality of different keys

2   and said steps of combining and transmitting comprises:

3   combining said encrypted data with each one of said plurality of

4   different keys in a plurality of broadcast messages; and

5   transmitting one of the plurality of broadcast messages to a

6   subset of said plurality of receiving nodes.

1   3.   The method of claim 2 wherein each one of said plurality of different

2   keys are associated with a category.

1   4.   A method for decrypting a message received over a broadcast

2   network comprising the steps of:

3   receiving data comprising an encrypted message and a hashed

4   key at a node in said broadcast network, wherein said node comprises

5   means for storing data;

6   parsing said data to derive said encrypted message and said

7   hashed key;

8   comparing said received hashed key with a plurality of keys

9   stored in said means for storing data in said node and to select a key

10   matching said received hashed key; and

11   decrypting said encrypted message with said matching key if a

12   match was found.

1   5.   The method of claim 4 further comprising the step of requesting a key

2   from a network entity.

1   6.   In a communications network having a plurality of network entities, a

2   first one of the network entities comprising:

3   a means encrypting data with a key;

4   a means for hashing said key;

5   a means for combining said encrypted data and said key in a

6   broadcast message; and

7   a means for transmitting said broadcast message to a plurality of

8   receiving nodes.

1   7.   The network entity of claim 5 further comprising a means for

2   distributing hashed keys.

8.   A computer-readable memory for directing a computer to function in a particular manner when used by the computer, comprising:

      a first portion to direct the computer to encrypt data with a key;

      a second portion to direct computer to hash said key;

      a third portion to direct computer to combine said encrypted data with said key in a broadcast message; and

      a fourth portion to direct computer to provide multiple transmissions of said message.

9.   A computer-readable memory for directing a computer to function in a particular manner when used by the computer, comprising:

      a first portion to direct the computer to receive data comprising an encrypted message and a hashed key;

      a second portion to direct computer to parse said data;

      a third portion to direct computer to compare said received hashed key with a plurality of keys and to select a key matching said received hashed key; and

      a fourth portion to direct computer decrypt said encrypted message with said matching key if a match was found and send request for key to a network entity if no matching key was found.

17

1   10.   A computer data signal embodied in a carrier wave, comprising an

2   encrypted message, a hashed key and instructions for:

3   parsing said data to derive said encrypted message and said

4   hashed key;

5   comparing said received hashed key with a plurality of keys

6   stored in said means for storing data in said node to select a key

7   matching said received hashed key; and

8   decrypting said encrypted message with said matching key if a

9   match was found and sending request for key to a network entity if no

10   matching key was found.

1   11.   A computer program product that enables a network entity distribute

2   secure content in a network comprising:

3   computer readable code that instructs computer to:

4   encrypt data with a key;

5   hash said key;

6   combine said encrypted data and said key in a broadcast

7   message;

8   transmit multiple transmissions of said broadcast message.

9   and

10   a tangible medium that stores the computer readable code.

1   12.   The computer product of claim 11 wherein the tangible medium is

2   selected from a group consisting of hard-disk, CD-ROM, DVD, floppy disk,

3   flash memory and the like.